Lunar Surface System Avionics Study Final Report

Ted Bonk

2/18/2009

LOCKHEED MARTIN

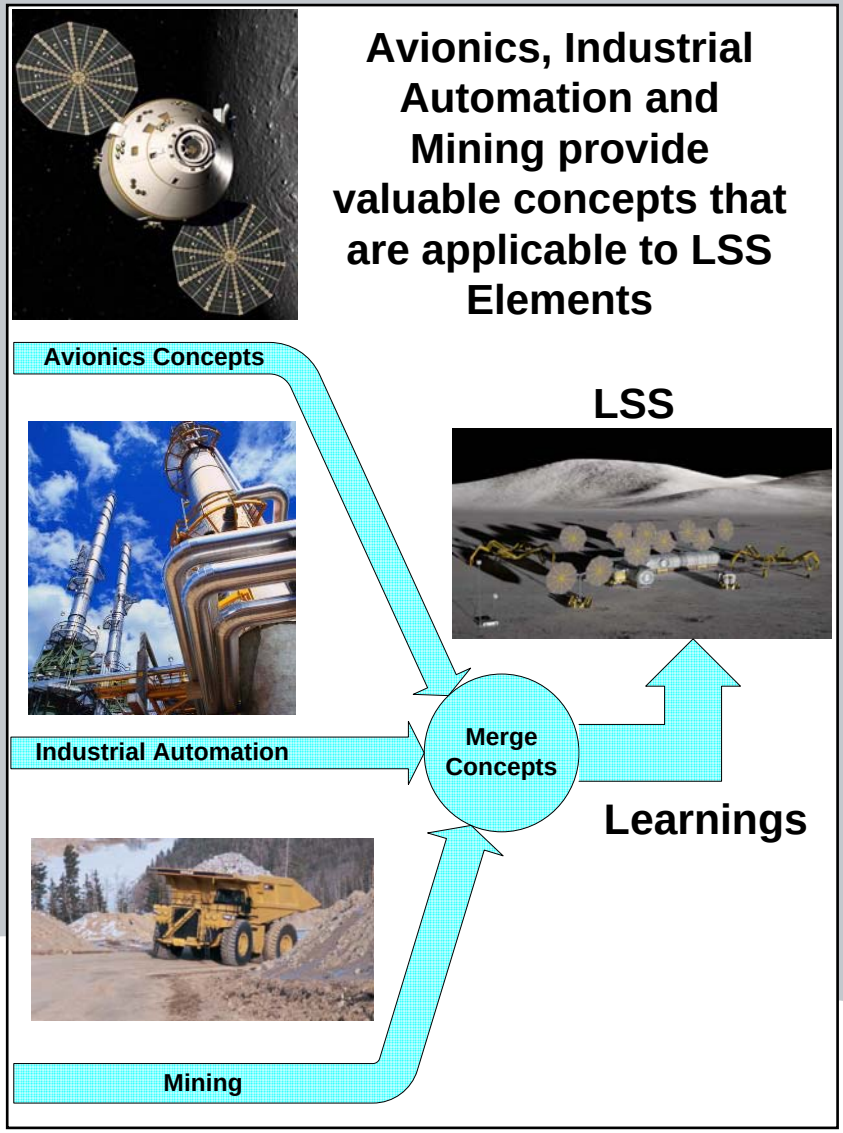
Honeywell

LSS Avionics Sparing Project Agenda

Honeywell

- Introductions (2 hours)
- Study Overview & Results
- Layered Electronics Architecture
  - Sensor/Effectors
  - Local Controllers
  - Supervisor Controller/Safety System
  - Data Buses
  - Functions
  - Software
  - Architecture Concepts
- Dynamic Commissioning
- Abnormal Situation Management
- Wireless Equipment
- Conclusion
- Q&A (15 min)

Study Overview & Results



LOCKHEED MARTIN

Honeywell

LSS Avionics Study C

Honeywell

- The objective of this stu…ate innovative avionics architectures and sparin… maximize commonality of avionics components …ilitate in-situ repair …s while minimizing mass of spares. Critical t… of sustainable avionics architecture are …eductions …ncluding indirect reductions via reductio… in power, …g, and maintenance spares.
- NASA stat…d the following as Technical Cl… the BAA:
  - S…erely mass constrained
  - … deployment to eventually coexist with subsequent generation …ware
  - Surface networks are highly sparse by must still be robust
- Here are the re-stated design drivers:
  - Minimize Power
  - Minimize Weight
  - Enhance Commonality (Common Spares) for Reuse/Salvage
  - Address Maintenance of Equipment
  - Maintain Composability & Extensibility

Industrial Automation Building/Mining Concepts in a Standard Framework

Fewer Spares & Unique Spares

Multi Vehicle Equipment

Integrated ISHM

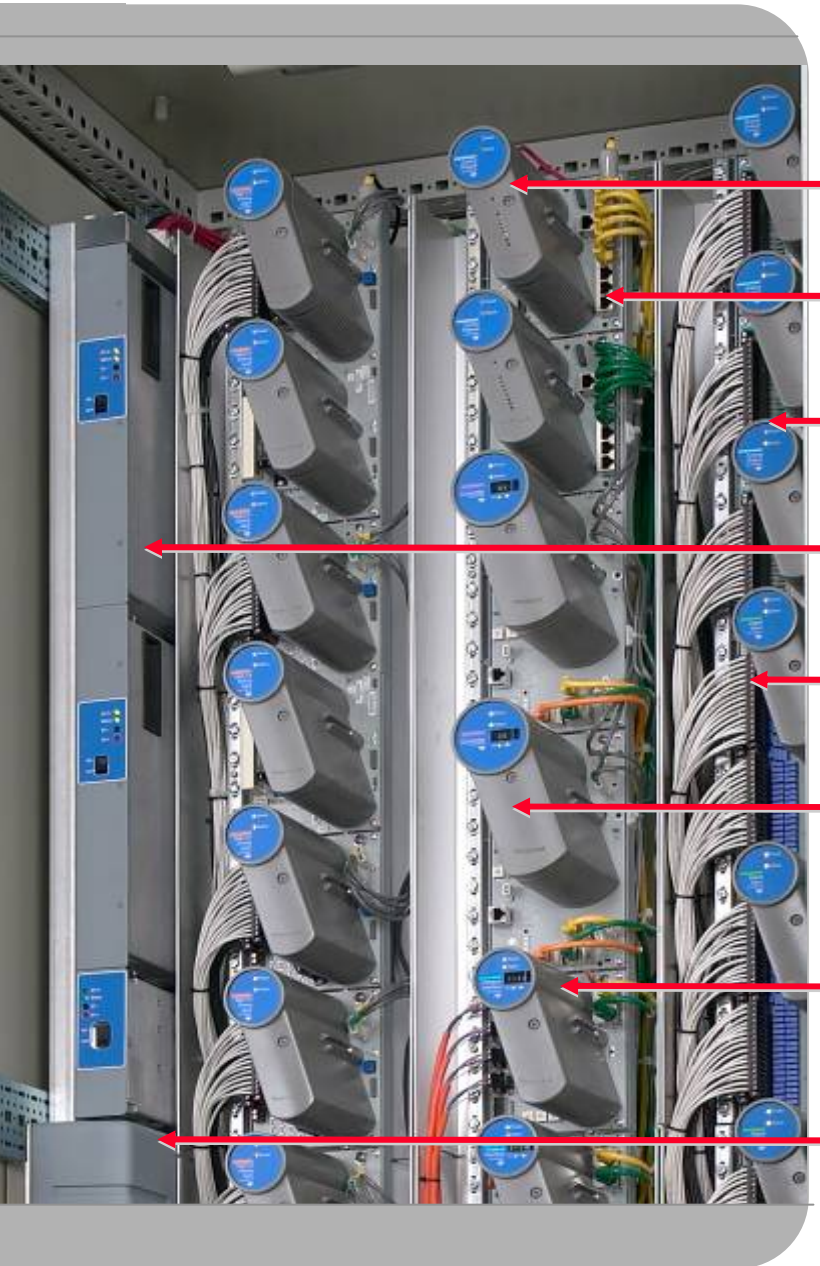
6th Generation Avionics & Sensor Stds

Dynamic Commissioning

ASM

Industrial Controller & IO Design Concepts

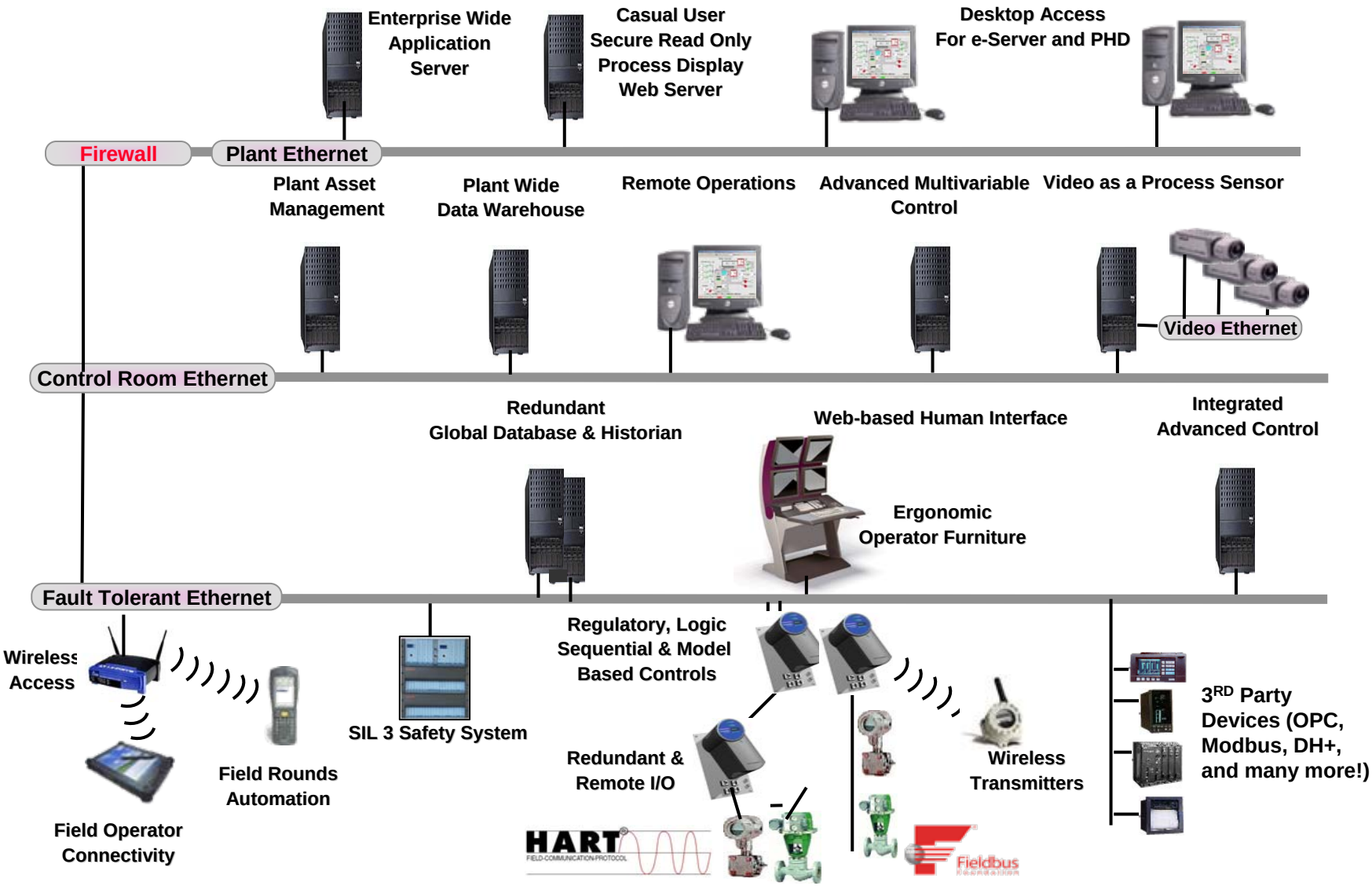
Honeywell



- Control Firewall
- Power Bus Bar
- Redundant Digital and Analog I/O
- Integrated Power Subsystem
- IO Rail
- Hotswap Processors & IO Modules
- Fieldbus Interface Module (IO)
- Batteries & Charger

Standard Industrial Control Architecture

Honeywell



Based on Reference Model for Computer Integrated Manufacturing, ISBN 1-55617-225-7

Lunar Control Platform Architecture (Quick Look)

Honeywell

Enterprise Wide Application Server

Casual User Secure Read Only Process Display Web Server
Public Access

Desktop Access For e-Server and PHD
Headquarters & Centers

Firewall

Plant Ethernet

Plant Asset Management
LSS Control

Plant Wide Data Warehouse
VAB

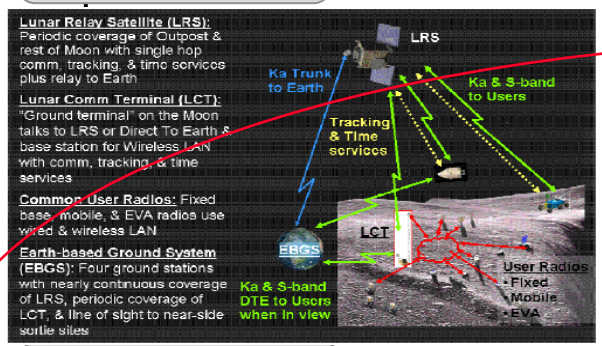
Remote Operations
Mission Control

Advanced Multivariable Control

Video as a Process Sensor
Launch Video

Video Ethernet

Control Room Ethernet



Redundant Global Database & Historian
Asset Management
HAB File System

Web-based Human Interface
LSS Control Center

Ergonomic Operator Furniture
HAB Furniture

Video as a Process Sensor
Intrusion Monitoring

Video Ethernet

Example Software Applications
Asset Manager
Video Manager
Boundary Management
Daily Instructions
Production Monitoring
Electronic Shift Log
Procedure Automation
Process Control & Monitoring

Fault Tolerant Ethernet

Wireless Access
LSS Wireless

Field Operator Connectivity
Rovers

Field Rounds Automation
Spacesuit

SIL 3 Safety System
Robotic Safety Partition

Regulatory, Logic Sequential & Model Based Controls

CSA

Redundant & Remote I/O

HART

FieldBus

Wireless Transmitters

3RD Party Devices (OPC, Modbus, DH+, and many more!)
Lunar Subsystems

Top Recommendations/Future Studies

Honeywell

Recommendations

1. Establish Programmatic Approach for Lunar Lander & LSS Electronics Commonality (Top Recommendation)
2. Establish a layered LSS Electronics Control Architecture across the vehicles
3. Establish Data Standards to allow data sharing & iinteroperability
4. IO Equipment/Power Control Integration

Suggested Future Studies

1. Sensor Type, Form Factor & Bus Standardization
2. LSS Equipment Health & Maintenance Approaches
3. Reconfigurable, Reusable LSS Software Architectures
4. Human Interface Standardization
5. Certification Standards
6. Altair and LSS Joint Avionics Development

Recommendation 1 Expansion

Honeywell

- **Programs that design equipment for application across multiple vehicles work when groundrules and direction are established at program onset**
- **Establish leader/follower with structured signoff to address programmatic issues**
  - **Structure procurement to allow/enforce commonality between programs across vehicles**
  - **Same requirements lead to different implementations without constant significant effort to bring implementations together**
  - **Procuring the same parts eliminates that effort**

“things that are different are not the same”

LSS
Layered Electronic Architecture

Common Electronics
Across the LSS Vehicles
(First Try)

LOCKHEED MARTIN

Honeywell

Architecture Overview Across the Vehicles

Honeywell

LSS Electronics Control Architecture Levels

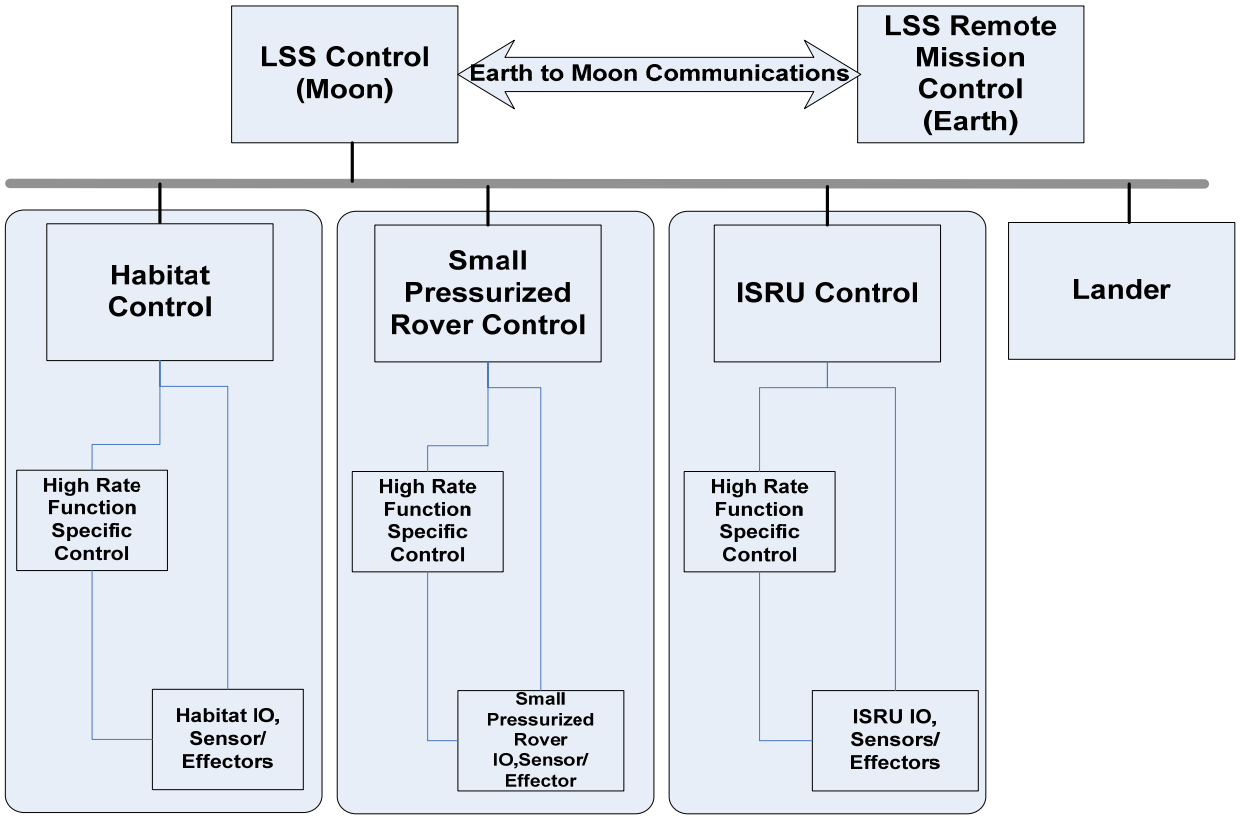
Level 3
- Production Mgmt
- Maintenance Mgmt
- Resource Mgmt

Level 2
Vehicle Control
- Sequencing
- Directing
- Coordinating

Health Status

Level 1
- High Rate Control
- Standard IO/ Power Control
- Standard Sensor/ Effectors

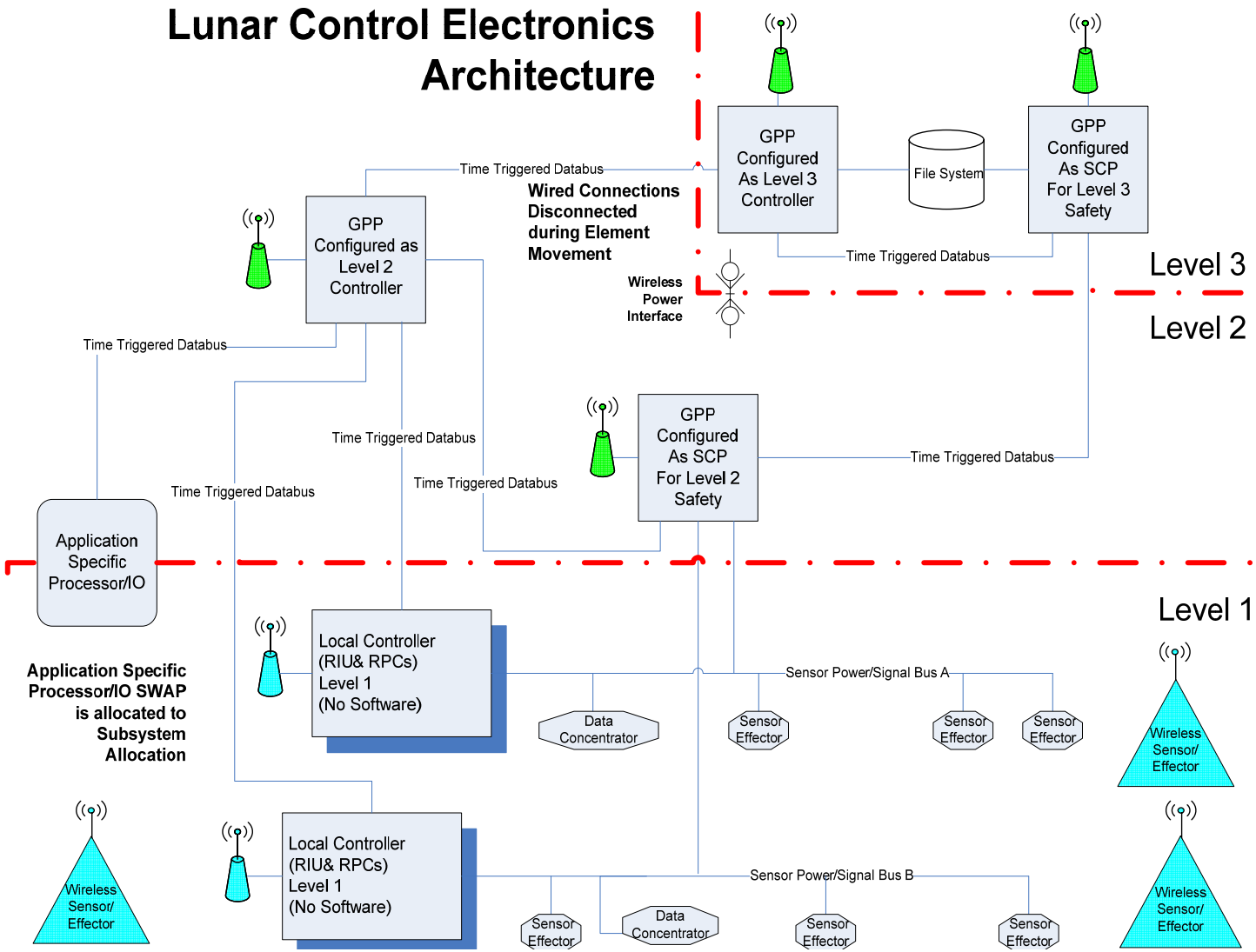
Standard Components
- Std Sensors/Effectors
- Data Concentrators
- Local Controllers
- Supervisor Controller/ Safety System
- Data Buses/Data Communications
- Functions
- Software
- File System



Enabled by standard functionality at each level with communications enabled by data standards

Electronic Architecture Components & Layers

Honeywell



Functions (Space & Industrial Automation Superset)

Honeywell

Level 3 Functions

Automation Control Functions

- Production Mgmt
- Daily Instructions
- Procedure Automation
- Production Monitoring
- Boundary Management
- Electronic Shift Log
- Maintenance Mgmt
- Procedure Automation
- Resource Mgmt
- Asset Manager
- Alarm System Analysis & Awareness
- Video Manager

LSS Functions

- Crew Health Monitoring and Medical Systems
- External Environment Monitoring and Protection
- Mission Planning and Operations
- Prognostics, Maintenance and Logistics Management

Level 2 Functions

Automation Control Functions

- Vehicle Control
- Sequencing
- Directing
- Coordinating
- Health Status
- Process Control & Monitoring

LSS Functions

- Command and Data Handling
- Communications & Tracking
- Crew Health Monitoring and Medical Systems
- Environmental Control and Life Support
- External Environment Monitoring and Protection
- Guidance Navigation and Control
- Remote and Autonomous Operation
- Surface Navigation
- Thermal Control
- Waste Management

Level 1 Functions

Characteristics

- High Rate Closed Loop Control
- Standard IO/Power Control
- Standard Sensor/Effectors

LSS Functions

- Power
- Mobility
- Crew Interface
- Lighting (Part of ECLS)

Recommendation 2 Impacts

Honeywell

Area	Recommendations	Impact
Sensor/Effector	Standardize Sensor/Effector	Fewer Spares
Sensor/Effector Buses	Use Sensor Buses	Less Wire Weight
Local Controller/Power Control	Non-Software Controller with 4-6 Card Types, power control & some flexible IO	Less Weight, Fewer Spares, Addresses Common Mode SW Faults & Exposure Time
Supervisor Controller/ Safety System	Create General Purpose Reconfigurable Processor for all vehicles	Less Weight, Fewer Spares, Lander Commonality
Databuses/Data Comm	Integrated Wired & Wireless	Flexibility, Wire Weight
Functions	Review Mining & Process Control Functions	Look for commonality between vehicles to reduce duplication
Software	Design Assurance Levels, Multiple SW Environments, Data Standards, Common Software	Reduced Cost, More Flexibility, Increased Safety
Architecture Capabilities	Implement basic and advanced architectural capabilities	Easier Upgrades, Maintenance, Safety
Program Structure	Implement Leader/Follower Program	Reuse of Lander Electronics

Sensor/Effectors & Sensor Buses

Honeywell

- Hundreds of sensors/effectors will be needed and maintenance drives the design
- Common Sensor/Effectors
  - Compact, Low Power
  - Easy Maintenance
  - Built-in RM
  - Employ self-packaging
  - Combined Signal & Power Communications
  - Wired & Wireless Versions
  - Common with Lunar Lander?
- Design them once and use on all vehicles and habitat
- Choose an Standard, Open combined Sensor/Effector Bus
  - Sensor Buses save wire weight
  - Address RM/Fault Isolation Aspects
- Altair study shows wiring can be 56% of Avionics weight
- Design them once and use on all vehicles and habitat

Embedded System Comparisons -- Input/Output

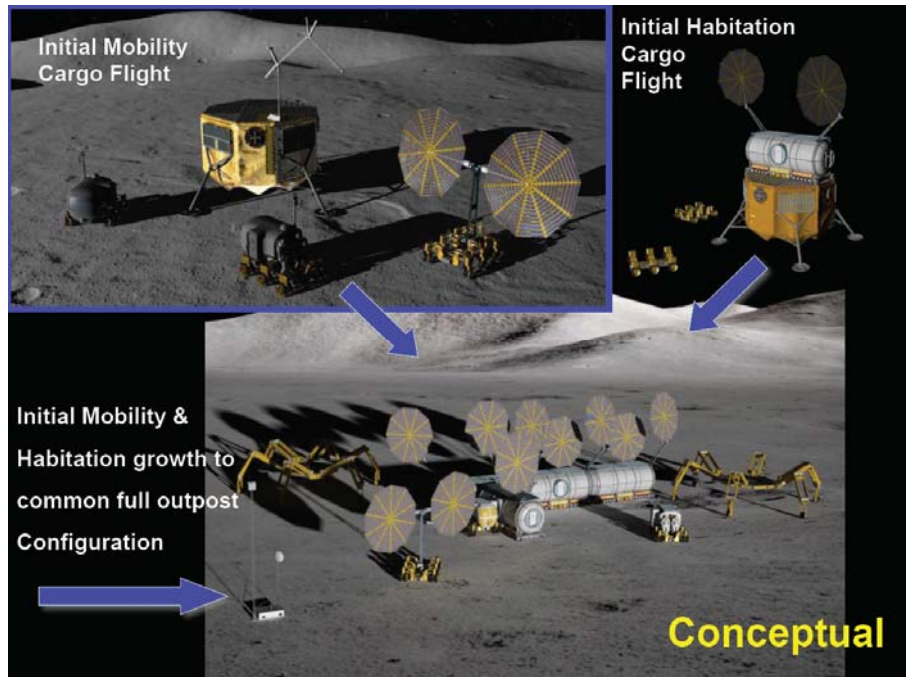
Honeywell

- **Vetronics (Airplanes, Spacecraft, Armored Personnel Carriers, etc.)**
  - **I/O is built into the vehicle**
    - I/O distribution is part of the vehicle design
    - Sensors and actuators are limited to save weight and power
- **Process Control and other Terrestrial Systems**
  - **Architectures are hierarchical**
    - Regulatory control levels use purpose-built controllers
      - Often redundant to provide availability in case of communications failures
      - May be located remotely to reduce latency in control loops
    - Supervisory and enterprise levels use commercial information technology equipment
      - Conventional IT assets and protocols with modifications for real-time performance and reliability
  - **Applications are I/O intensive**
    - Some process applications have > 20,000 sensors/actuators
      - Sensors and actuators may be distributed over several miles
    - I/O usually is wired directly to controllers (“home run” wiring)
    - Newer equipment uses multi-drop buses for economy and ease of commissioning
      - Based on standard protocols such as Foundation Fieldbus, Profibus, LONworks, some Modbus
  - **I/O is commissioned in the field**
    - Older equipment requires manual configuration
      - Device addresses, data ranges and register assignments are manually set during installation
    - Newer equipment provides automatic discovery to minimize field labor
      - Device characteristics are sent by the device on connection
      - Device addresses are dynamically assigned by controllers
- **Lunar Surface System**
  - **I/O architecture uses vehicle assets to implement a terrestrial I/O architecture**

Local Controllers (Data & Power Control Integ)

Honeywell

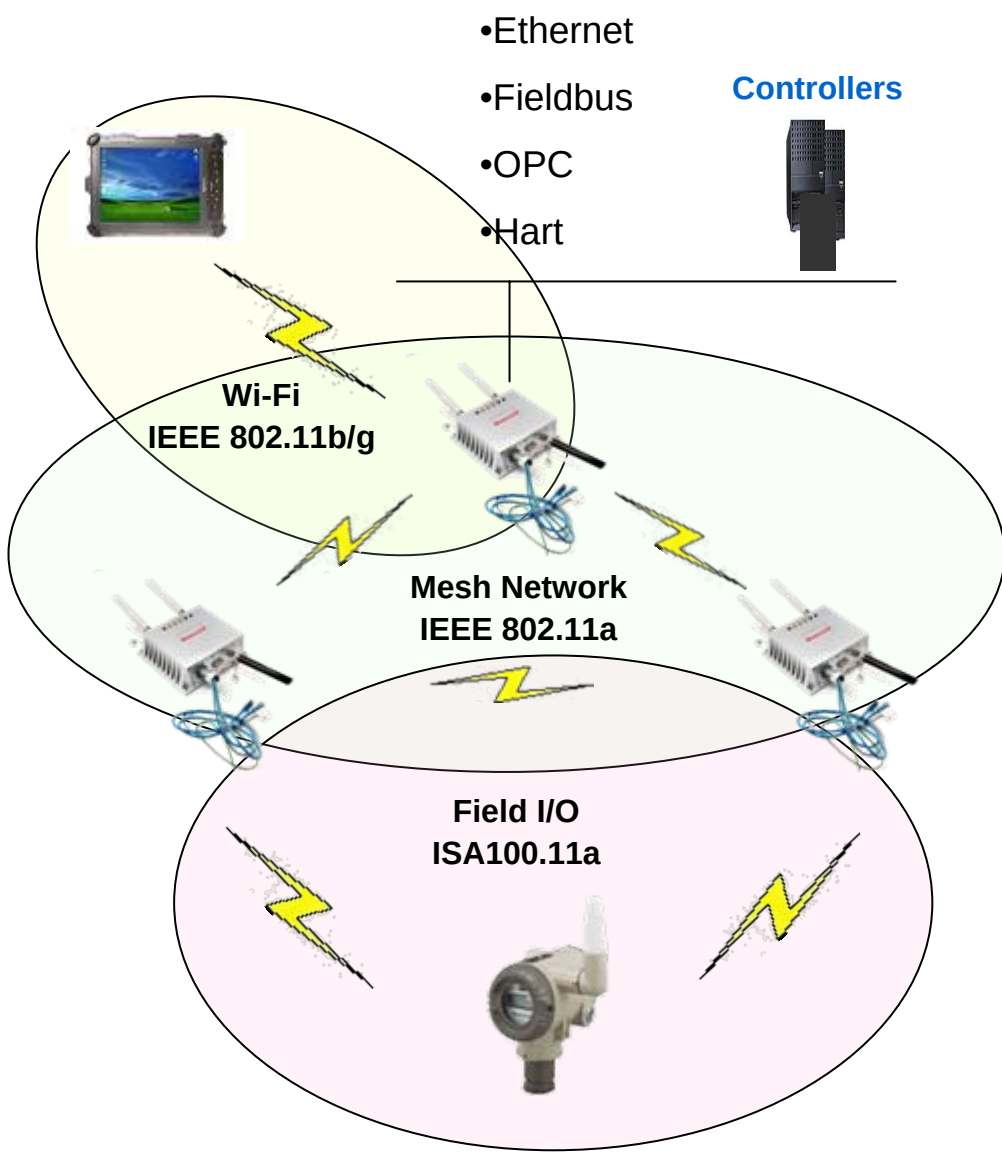
- **Integration Level of Control & Power**
  - Reduces Size, Weight, Power & LCC
- **Local Controller (PDU Like)**
  - 4-6 Circuit Card Types for Signal & Power
  - Hardware Based Controller due to Common Mode SW Faults & Exposure Time
- **Design them once and use on all vehicles and habitat**



Data Buses/Data Communications

Honeywell

- **Integrated Wired & Wireless Communications**
- **Time Triggered Protocols**
- **Ethernet Compatible**
- **Space Qualified Wireless Parts**
- **Design them once and use on all vehicles and habitat**



Supervisor Controller/Safety System

Honeywell

- General Purpose Computer
  - Reconfigurable Processor
  - Network Switch
  - Wireless Capability
- GPP as Level 2/3 Controller
- GPP as Safety System with different simpler software
- Design them once and use on all vehicles and habitat

Software

Honeywell

- **Recommendation Software-1**

  Establish and use multiple assurance levels for software design, verification and qualification processes to support these levels. This is to reduce initial software cost as well as maintenance costs by only doing the effort as required by the safety analysis

- **Recommendation Software-2**

  Establish standard software architectures, supporting services and execution environment for all LSS elements supporting: Hard Real-time Environment, Software Real-time Environment and Windows-like or equivalent. This is to allow for software to be developed and hosted in an environment best suited for that application (GN&C in Hard Real-Time & Excel in Windows type OS)

- **Recommendation Software-3**

  Establish common software repositories to eliminate replication of software pieces for multiple vehicles. This is to reduce cost and increase quality by exposing building blocks to wider use and implicit testing.

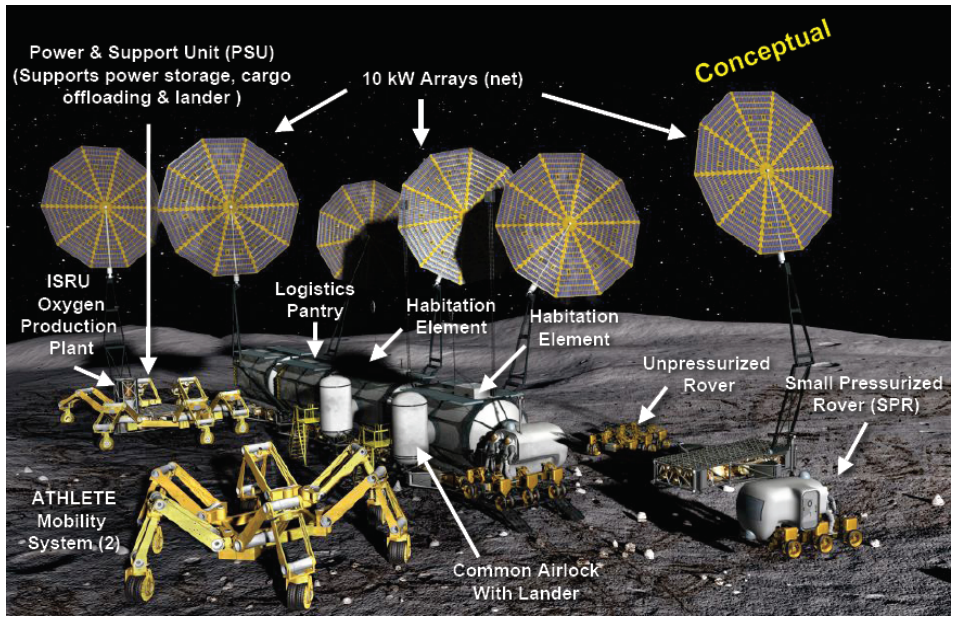
- **Recommendation Software-4**

  Establish data standards for communications between software in the different sensors, effectors, computing unit (e.g. expansion of OPC - OLE for Process Control to include common vocabulary/taxonomy/ontology). This is to allow for remote data access to remote equipment and reduce IO software development costs.

Architecture Capabilities

Honeywell

- **Basic Capabilities**
  - Defined roles & responsibilities per layer with defined interfaces to enable upgrades
  - Interfaces that meet open standards to facilitate Third Party Hardware & Software Integration
  - Allow for vehicle unique functions/electronic but required justifications and allocate costs



- **Advanced Capabilities**
  - Hot Swap & Dynamic Upgrades
  - Integrated System Health Management (ISHM)
  - Reconfigurable Computing
  - Abnormal Situation Management
  - Dynamic Commissioning

Advanced Capability – System Commissioning

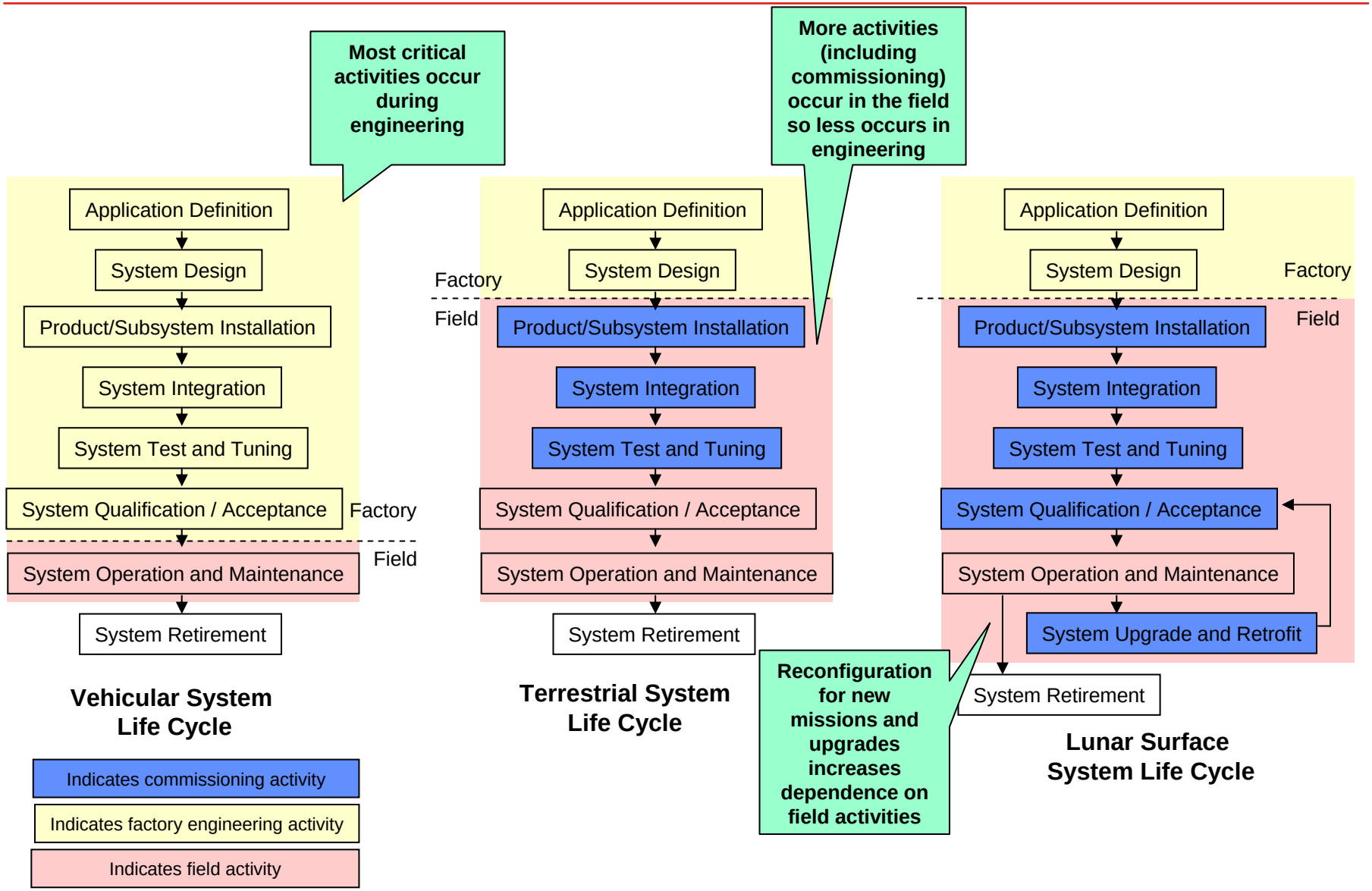
Honeywell

- **Adapts a system to a specific field environment**
  - **Installs and configures components to field constraints**
    - Installs sensors and actuators
    - Installs communications and power wiring
    - Sets computer parameters and drivers for field devices
    - Inventories devices and configures device addresses and parameters
    - Installs application software and tunes application parameters
  - **Tests system operation**

- **Typically the last step before operational status**
  - **Always performed in the field**
  - **Verifies the system meets user needs**
  - **Must be repeated if major system changes or upgrades occur**

LSS Shifts Commissioning Activities to the Field

Honeywell



Advanced Capability – Dynamic Commissioning

Honeywell

- **Extends conventional system commissioning to support evolving field operations in a remote environment**
  - **Provides flexibility to adapt to changing conditions**
    - Build-out of lunar habitations and communications
    - Mission evolution
  - **Uses standard and reusable components to minimize field configuration effort**
    - Standard computers for economy and interchangeability
    - Multi-purpose I/O architecture for flexibility
    - Standard sensors and actuators for simplicity and reuse
    - Prewired I/O to simplify hardware installation
    - Dynamic device discovery and configuration to minimize manual configuration of device addresses and parameters
    - Standard communications to minimize time spent in harsh environments
  - **Supports commissioning with software**
    - Unified database of process points to manage data aggregation and distribution
    - Automated discovery and provisioning software to eliminate manual data entry
    - Standardized software for data visualization and control

Abnormal Situation Management

Honeywell

- An abnormal situation is a disturbance or series of disturbances in a system with which the control system is unable to cope, and which requires operator intervention.
- Abnormal Situation Management, like general emergency management, is achieved through Prevention, Early Detection, and Mitigation of abnormal situations, thereby reducing unplanned losses that can include lost time, loss of equipment, or loss of life.
- The "Paradox of Automation" is that the very automation we design to manage complexity may reduce the operator's awareness and limit opportunities to reinforce their knowledge. When the automated system is unable to handle a problem the operator may lack the situation awareness or skill required to for correct intervention.

"In systems where a high degree of hardware redundancy minimizes the consequences of single component failures, human errors may comprise over 90% of the system failure probability."

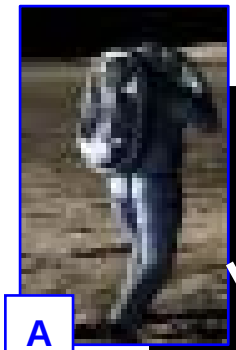
"A Manager's Guide to Reducing Human Errors" API Publication 770, March 2001

Recipe for Disaster

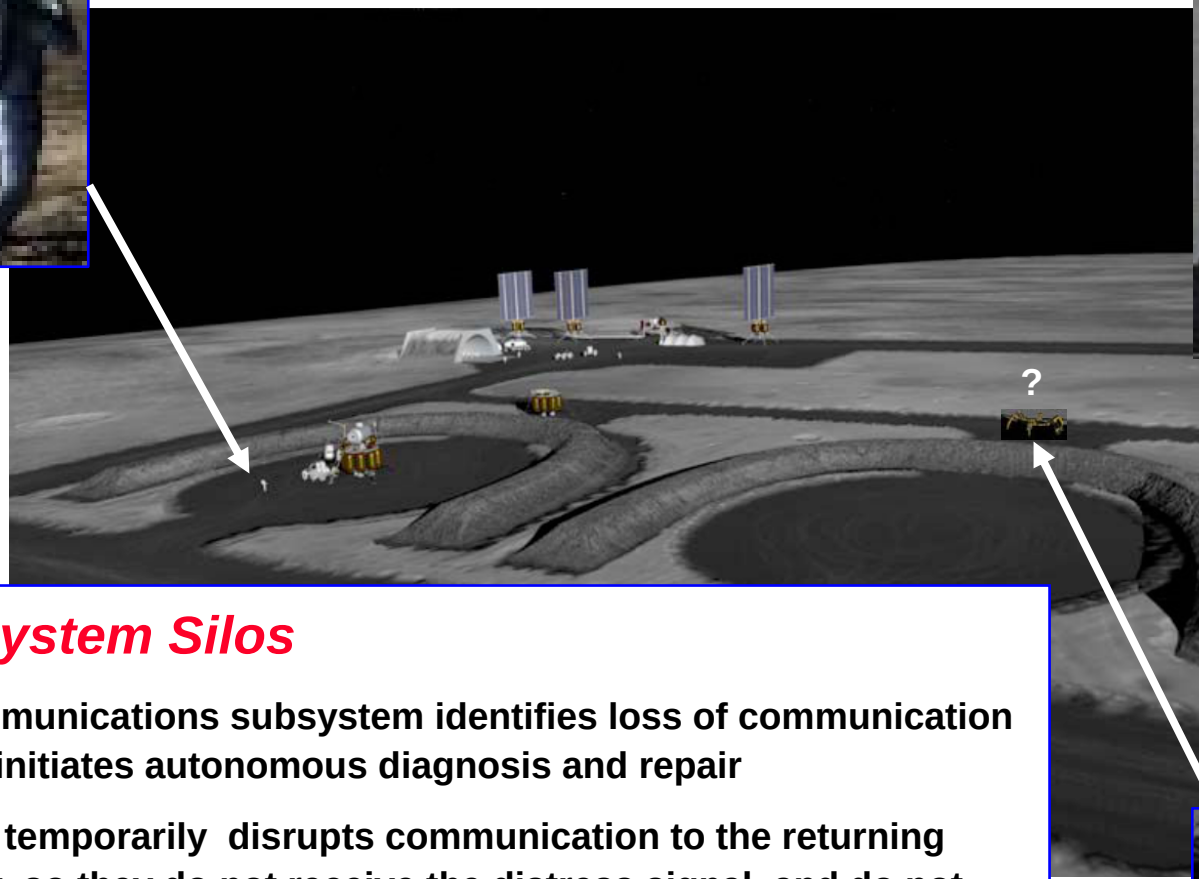
Honeywell

Returning Crew – Low O_2

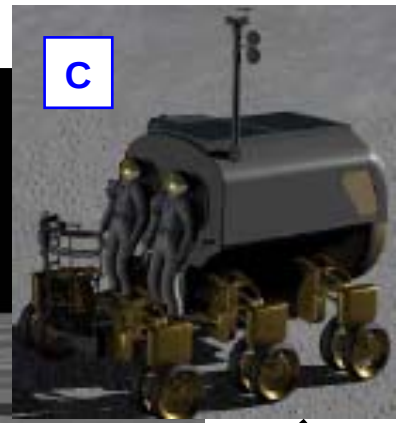
Crew member in EVA in distress



A



C



B

Tri-Athlete
(Lost Communication)

Sub-System Silos

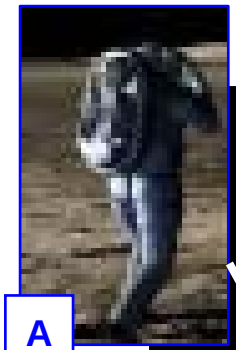
C Communications subsystem identifies loss of communication and initiates autonomous diagnosis and repair

B This temporarily disrupts communication to the returning crew, so they do not receive the distress signal, and do not know their shortest route is blocked

A The disabled crew member is put at high risk

Shared Situation Awareness

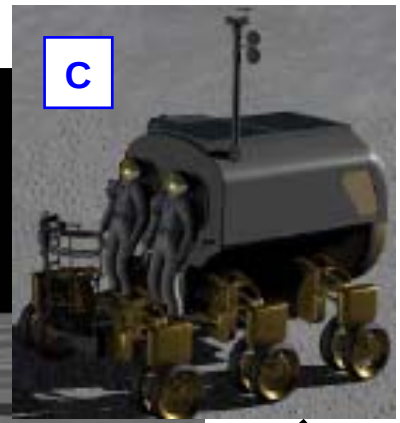
Honeywell



Crew member in EVA distress

A

Returning Crew – Low O_2



C

?

B

Tri-Athlete
(Lost Communication)

Resource Optimization

- **A** The crewmember in EVA distress has highest priority
- **C** The communications subsystem holds requests unrelated to mobile crews and related vehicles
- **B** The returning crew is routed to the landing area where they can access oxygen reserves and assist the distressed crewmember

Benefits of ASM and Human-Centered Design

Honeywell

- **In the environment of a lunar mission there is a staggering array of systems and personnel who are likely to be operating simultaneously to achieve *potentially* conflicting goals.**
- **ASM design principles address the human-in-the-loop in a comprehensive manner**
  - **appropriate context sharing and common understanding of the hierarchy of goals and threats**
  - **appropriate separation of concerns (environment, transport, research work product) with carefully arbitrated rules of priority**
  - **resource optimization through well arbitrated human and automation collaboration**

In the design of the lunar base, the human is the most variable, unpredictable, and intractable component within the control network.

Wireless Sensors & Effectors

Safety

Eliminate Hazards

$20B losses per year in US Petrochem Industry

Reliability

Reduce Downtime

Millions lost per year due to unplanned production losses

Efficiency

Reduce Costs

Improve Productivity

Ease of Installation

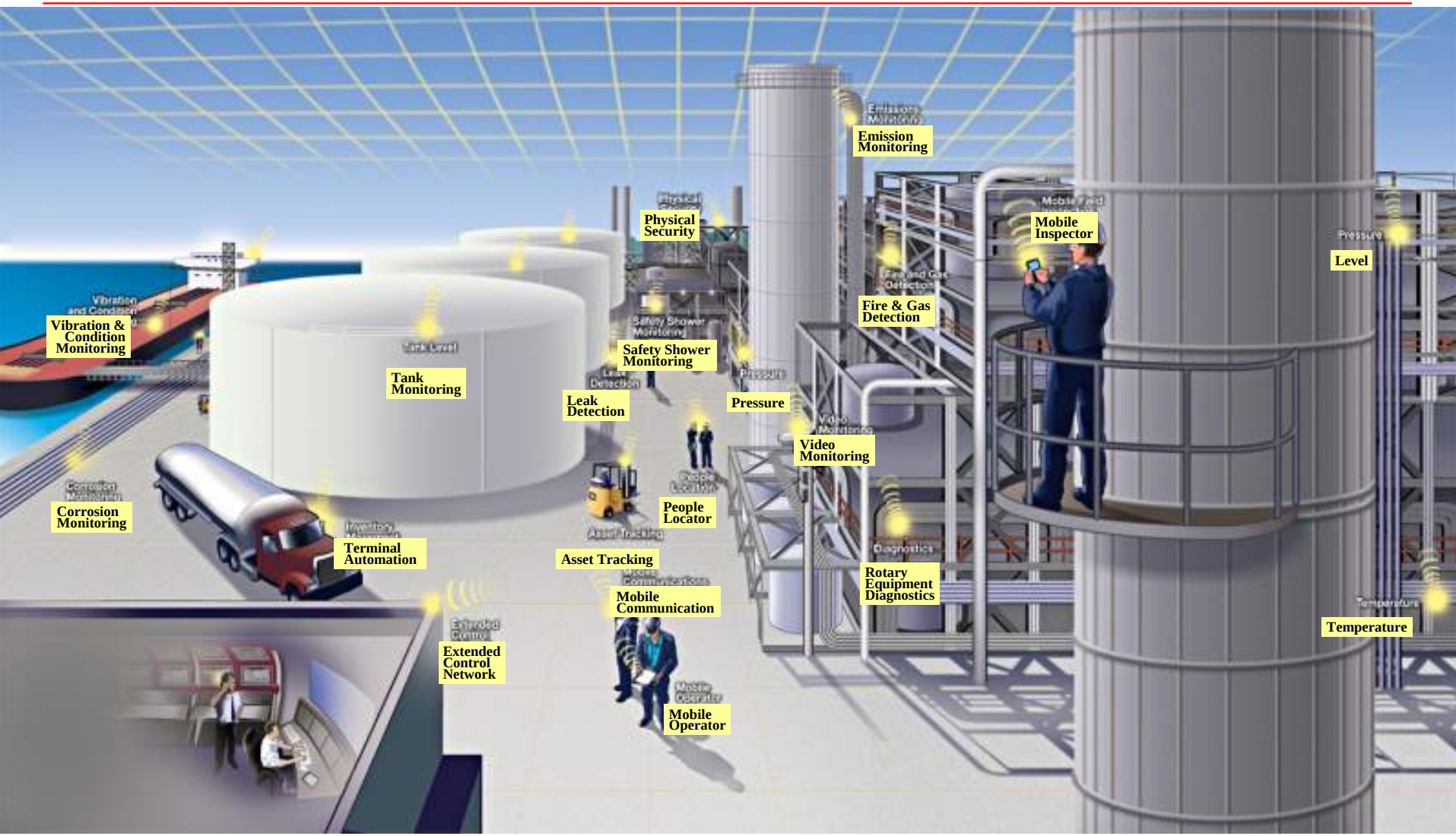
Process optimization

LOCKHEED MARTIN

Honeywell

Wireless Sensors in a Refinery (Find the LSS Parallels)

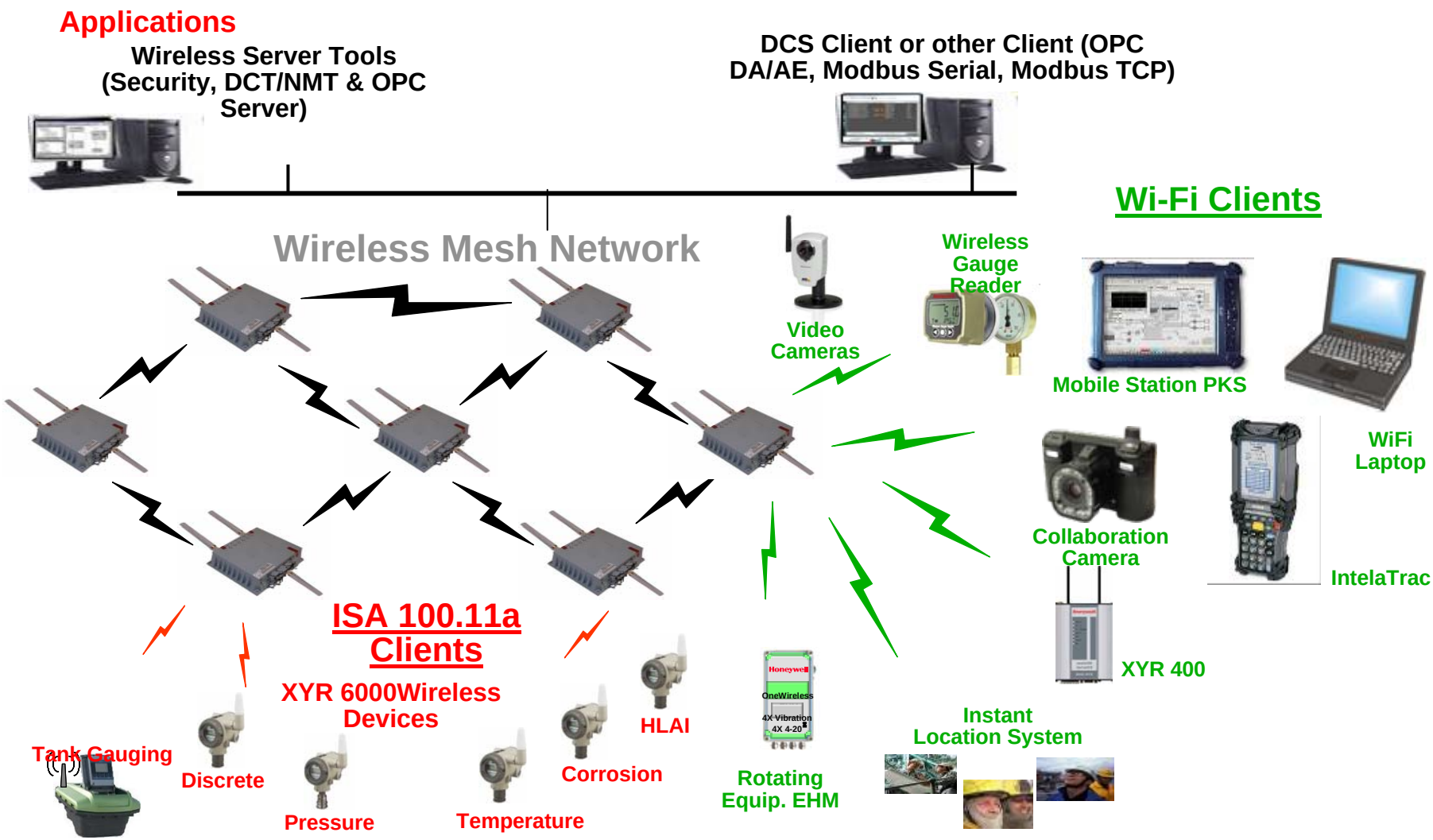
Honeywell



DOE Contract: Wireless and Sensing Solutions for Improved Industrial Efficiency
Honeywell Project: Wireless Networks for Secure Industrial Applications

Four Networks (3 Wireless, 1 Wired) Tied Together

Honeywell



Wireless Equipment Specifications

Honeywell

MultiNodes/Mesh

- **Capacity**
  - **22 Multinodes Per Mesh**
  - **100 Transmitters/Gateway**
  - **2200 Transmitters/Mesh**
- **Classifications**
  - **Class I Div 2**
- **Power**
  - **24VDC Power**
  - **110 VAC Power Supply Available**
  - **Solar Power Options**
- **Range**
  - **Up to 3000 ft from Multinode**
    - Further Distances with Directional Antennas
- **Antennas – Standard Omni-Directional, Directional, High-Gain and Remote**
- **Operating temperature: - 40° to + 75°C**
- **Interfaces**
  - **Configurable Modbus TCP Server**
  - **HART Gateway**

Sensors Transmitters

- **Types**
  - **Pressure**
  - **Differential Pressure**
  - **Temperature**
  - **Corrosion**
  - **HLAI (High Level Analog Input)**
  - **Discrete Inputs**
- **Classifications**
  - **Class I Div I**
- **Battery Life**
  - **Up to 10 Years**
- **Range**
  - **Up to 2000 ft from Multinode**
- **Reporting Rate**
  - **1, 5, 10 and 30 Second Reporting**
- **Antennas – Standard Omni-Directional, Directional, High-Gain and Remote**
- **Operating temperature: - 40° to + 75°C**

Conclusions

LOCKHEED MARTIN

Honeywell

Conclusions

Honeywell

- We expected to find a level of synergy and we were surprised by the amount and applicability.
- Industrial Automation, Building Control and Mining Industries have many applicable technologies/concepts for LSS
  - In some case, the technologies are further advanced than in Aerospace (Wireless Sensors & Sensor Buses)
  - Not everything is directly applicable due to size, weight & environment but these are workable
- Using the combination of knowledge, we answered the BAA questions, made recommendations and suggested studies/technologies, programatic suggestions

The real strength came from combining concepts and capturing lessons learned from multiple industries --

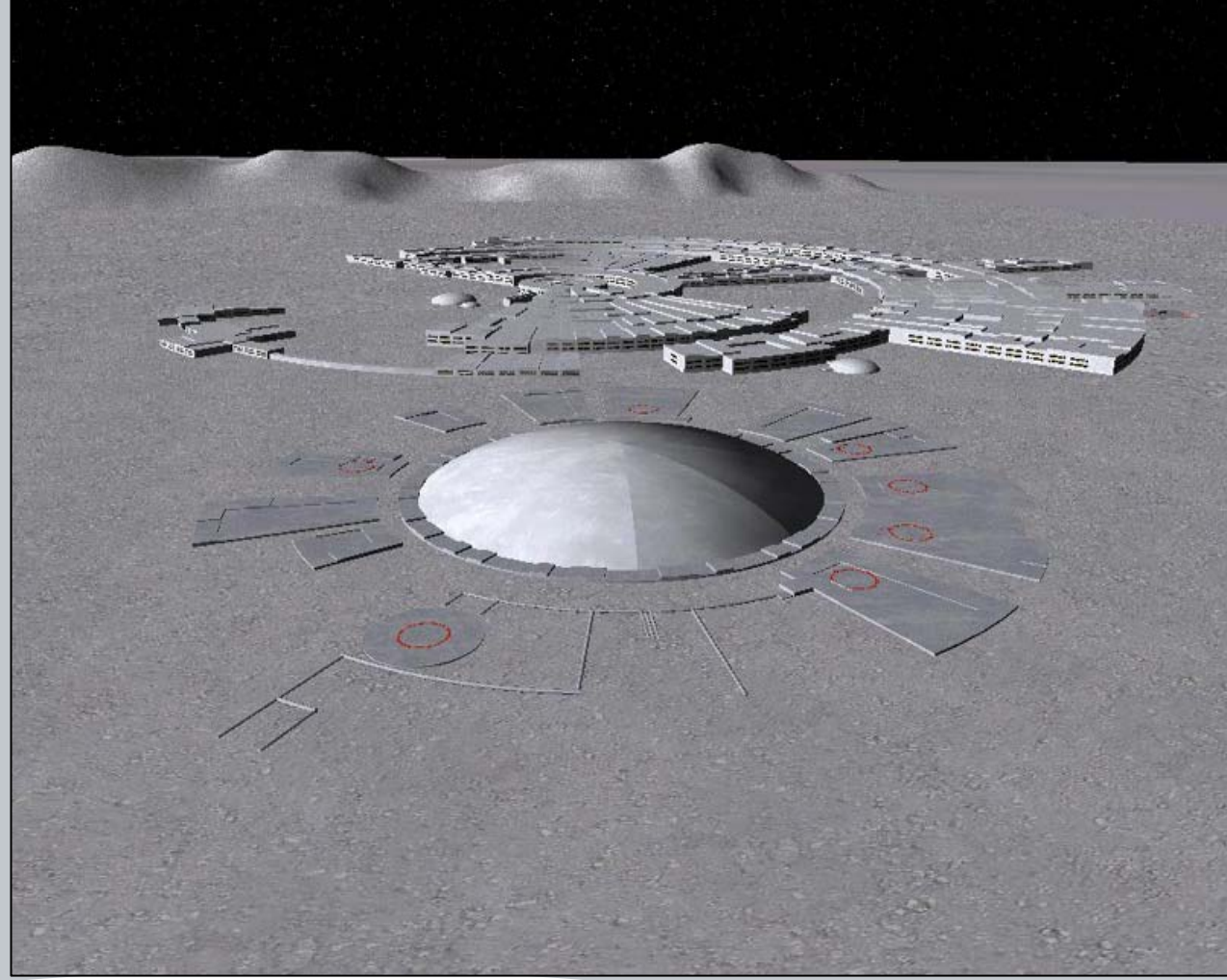
No one has the market cornered on good ideas.

Questions

LOCKHEED MARTIN

Honeywell

Backup



Honeywell

Technology Needs

LOCKHEED MARTIN

Honeywell

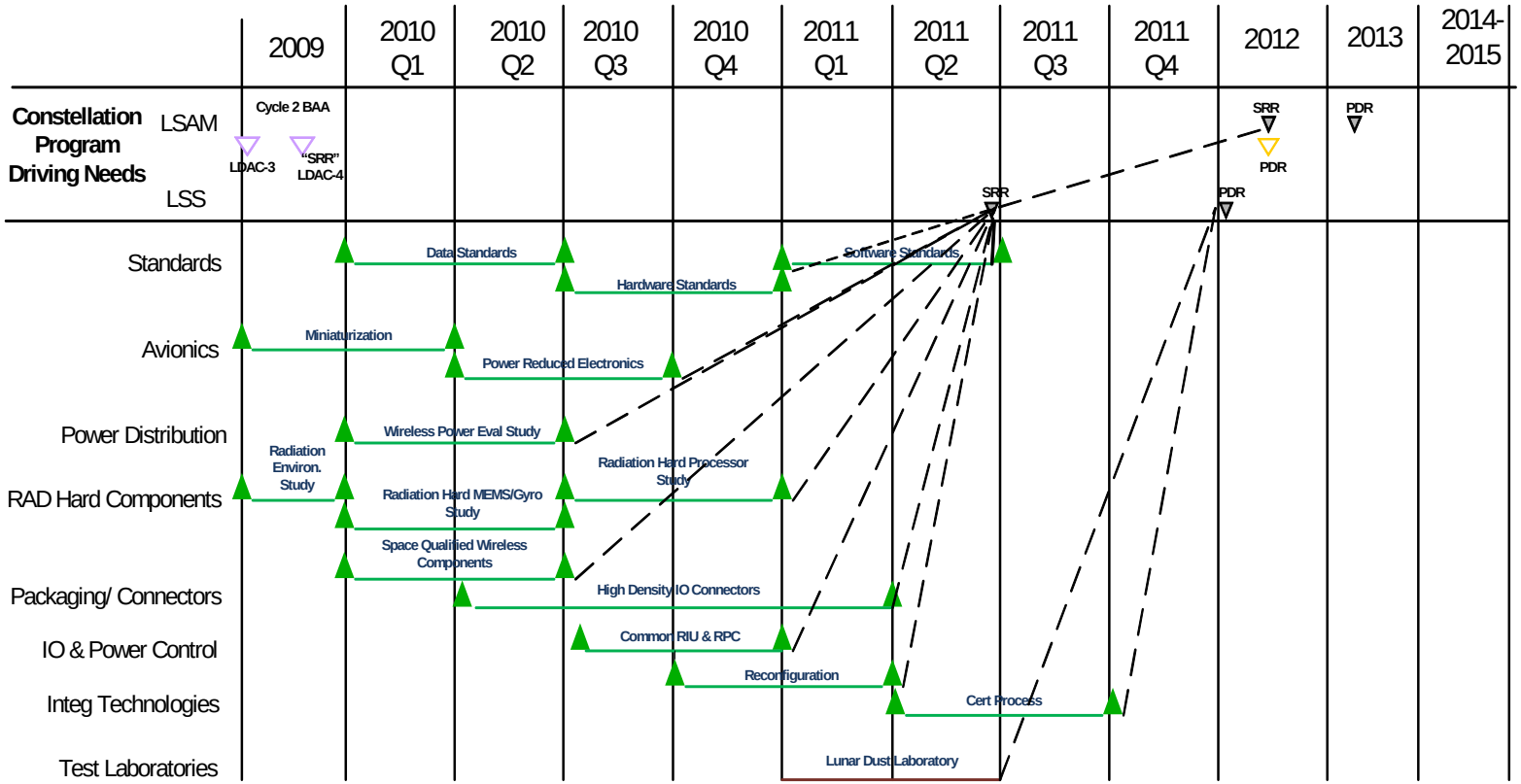
Technology Roadmap

Honeywell

NASA TECHNOLOGY CHALLENGES

Weight	Power
Commonality	Reusability
Integrated Maintenance	Salvage
Composability	Extensibility

Avionics Equipment
- Processing Elements & Networks
- Integrated IO/Power Control
- Dust Proof Connectors
- Nav. Components



Legend:
- Milestone
- Decision

Study Type:
- BAA
- Other
- Parts
- Customer
- Capital
- Program

POTENTIAL APPLICATIONS
- Lunar Habitat
- Chariot Crew Mobility Chassis
- Pressurized Rover
- Power and Support Unit
- Heavy-Lift Mobility

Purdue Reference Model

Honeywell

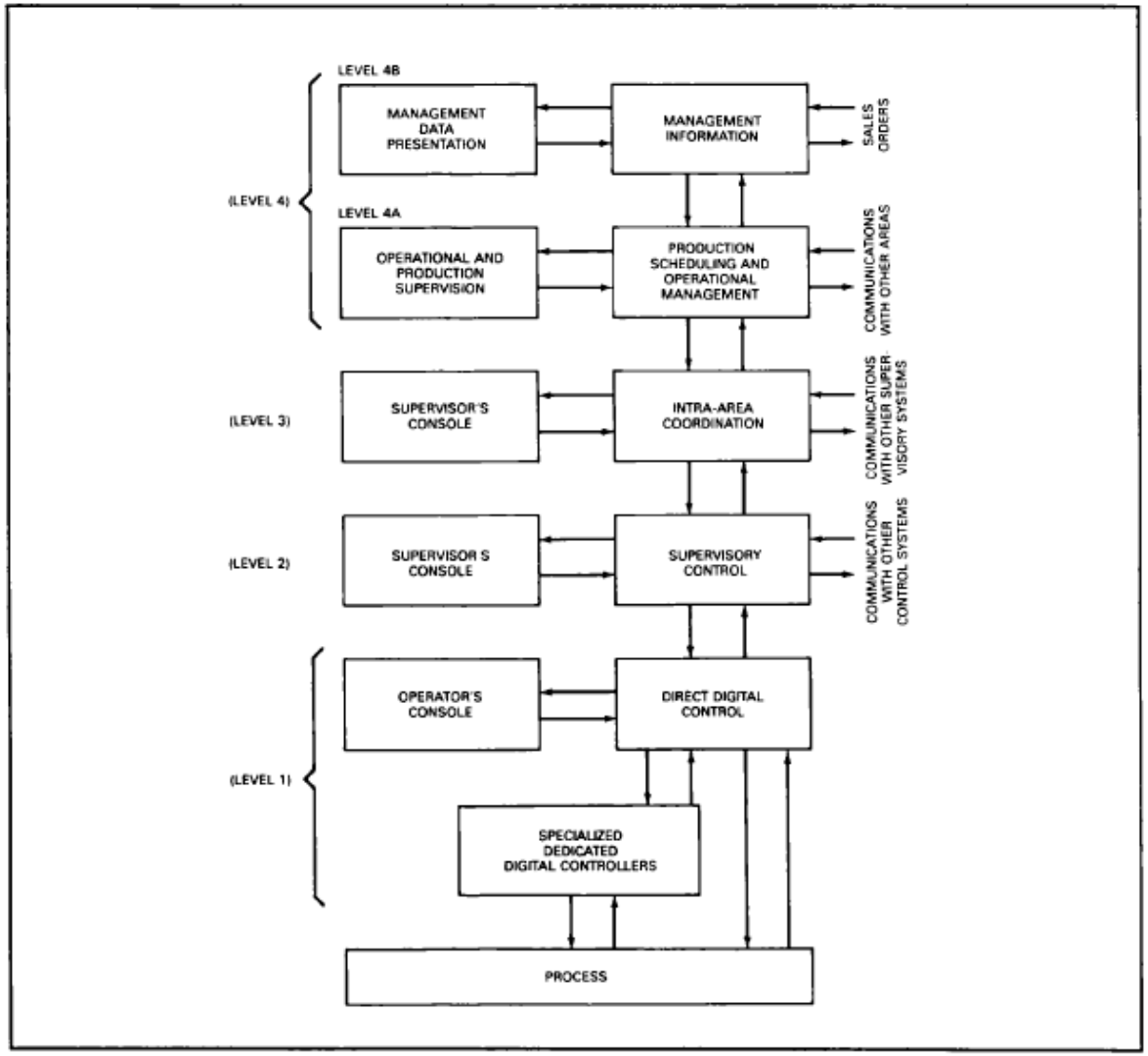


Figure 3-1 Assumed functional hierarchical computer control structure for an industrial plant (continuous process such as petrochemicals).

A Reference Model for Computer Integrated Manufacturing, ISBN 1-55617-225-7

Purdue Model Responsibility

Honeywell

IPW LEVEL NOTATION	WG1 LEVEL	HIERARCHY	CONTROL	RESPONSIBILITY	BASIC FUNCTIONS	
NULL	6	ENTERPRISE	CORPORATE MANAGEMENT	Achieving the mission of the enterprise and managing the corporate	— CORPORATE MANAGEMENT — FINANCE — MARKETING & SALES — RESEARCH & DEVELOPMENT	CONSIDERED AN EXTERNAL ENTITY IN THE IPW WORK
4	5	FACILITY/ PLANT	PLANNING PRODUCTION	Implementation of the enterprise functions, and planning and scheduling the production	— PRODUCT DESIGN & PRODUCTION ENGINEERING — PRODUCTION MANAGEMENT (Upper Level) — PROCUREMENT (Upper Level) — RESOURCES MANAGEMENT (Upper Level) — MAINTENANCE MANAGEMENT (Upper Level)	
3	4	SECTION/ AREA	ALLOCATING AND SUPERVISING MATERIALS & RESOURCES	Coordinate the production and supporting the jobs and obtaining and allocating resources to the jobs	— PRODUCTION MANAGEMENT (Lower Level) — PROCUREMENT (Lower Level) — RESOURCES MANAGEMENT (Lower Level) — MAINTENANCE MANAGEMENT (Lower Level) — SHIPPING — WASTE MATERIAL TREATMENT	
2	3	CELL	COORDINATE MULTIPLE MACHINES AND OPERATIONS	Sequencing and supervising the jobs at the shop floor, and supervising various supporting services	— SHOP FLOOR PRODUCTION (Cell Level)	
1	2	STATION	COMMAND MACHINE SEQUENCES AND MOTION	Directing and coordinating the activity of the shop floor equipments	— SHOP FLOOR PRODUCTION (Station Level)	
0	1	EQUIPMENT	ACTIVATE SEQUENCES AND MOTION	Realization of commands to the shop floor equipments	— SHOP FLOOR PRODUCTION (Equipment Level)	NOT INCLUDED BECAUSE OF WIDE DIFFERENCES OF EQUIPMENT AND FUNCTIONS BETWEEN DIFFERENT INDUSTRIES

Figure 3-4 Factory automation model.

A Reference Model for Computer Integrated Manufacturing, ISBN 1-55617-225-7

Honeywell

www.honeywell.com